

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Yasutaka SATO
Title: MODEM DEVICE, DATA
COMMUNICATIONS SYSTEM,
METHOD OF AND DEVICE FOR
PROTECTING DATA AND
COMPUTER PRODUCT



Appl. No.: Unassigned

Filing Date: August 9, 2001

Examiner: Unassigned

Art Unit: Unassigned

CLAIM FOR CONVENTION PRIORITY

Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application filed in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed.

In support of this claim, filed herewith is a certified copy of said original foreign application:

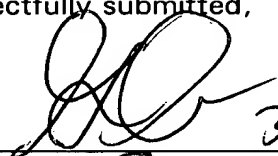
- Patent Application No. 2000-244537 filed 08/11/2000.

Respectfully submitted,

Date August 9, 2001

FOLEY & LARDNER
Washington Harbour
3000 K Street, N.W., Suite 500
Washington, D.C. 20007-5109
Telephone: (202) 672-5332
Facsimile: (202) 672-5399

By

 34371
Kenneth E. Krosin
Attorney for Applicant
Registration No. 25,735

Best Available Copy

日本国特許庁
JAPAN PATENT OFFICE

J1046 U.S.
09/924585
08/09/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2000年 8月11日

出願番号

Application Number:

特願2000-244537

出願人

Applicant(s):

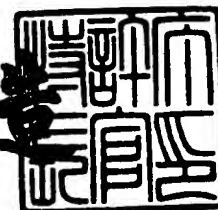
株式会社トリニティーコミュニケーション

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 7月27日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造



出証番号 出証特2001-3067478

Best Available Copy

【書類名】 特許願

【整理番号】 TC00-003

【提出日】 平成12年 8月11日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 徳島市川内町平石住吉209番地5 株式会社トリニティーコミュニケーション内

【氏名】 佐藤 泰崇

【特許出願人】

【識別番号】 300023383

【氏名又は名称】 株式会社トリニティーコミュニケーション

【代理人】

【識別番号】 100104190

【弁理士】

【氏名又は名称】 酒井 昭徳

【手数料の表示】

【予納台帳番号】 041759

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0003907

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ防護処理装置、モデム装置、データ通信システム、データ防護処理方法、その方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

【特許請求の範囲】

【請求項1】 連続するデジタルデータを順次読み込み、読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理手段と

前記判定処理手段によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項2】 シリアル入力されたバイナリデータをバイトデータに変換して一時的に保持する保持手段と、

前記保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

前記演算処理手段によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項3】 シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持手段と、

前記保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理手段と、

前記データ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判

定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、

前記演算処理手段によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理手段と、

前記データフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項 4】 前記演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 1～3 のいずれか一つに記載のデータ防護処理装置。

【請求項 5】 連続するデジタルデータである送信データ／受信データを順次読み込み、読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第 1 の演算処理手段と、

連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項 6】 シリアル入力されたバイナリデータである送信データ／受信

データをバイトデータに変換して一時的に保持する第 1 の保持手段と、

前記第 1 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理手段と、

前記第 1 の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第 1 の出力手段と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して一時的に保持する第 2 の保持手段と、

前記第 2 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、

前記第 2 の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第 2 の出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項 7】 シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第 1 の保持手段と、

前記第 1 の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第 1 のデータ抽出処理手段と、

前記第 1 のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードで

あると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理手段と、

前記第 1 の演算処理手段によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第 1 のデータフレーム再構成処理手段と、

前記第 1 のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第 1 の出力手段と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第 2 の保持手段と、

前記第 2 の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第 2 のデータ抽出処理手段と、

前記第 2 のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と

前記第 2 の演算処理手段において減算／加算されたバイトデータをもちいてデータフレームを再構成する第 2 のデータフレーム再構成処理手段と、

前記第 2 のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第 2 の出力手段と、

を備えたことを特徴とするデータ防護処理装置。

【請求項 8】 前記第 1 および第 2 の演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 5～7 のいずれか一つに記載のデータ防護処理装置。

【請求項 9】 さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、

前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、

を備えたことを特徴とする請求項 1 ～ 8 のいずれか一つに記載のデータ防護処理装置。

【請求項 1 0】 送信するデジタルデータに対して、標準化されたデータ圧縮規格に基づいてデータ圧縮処理を施すデータ圧縮手段と、

前記データ圧縮手段によってデータ圧縮処理を施されたデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して所定の演算値を加算／減算する第 1 の演算処理手段と、

前記第 1 の演算処理手段において加算／減算されたバイトデータを出力する第 1 の出力手段と、

受信したデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して前記所定の演算値を減算／加算する第 2 の演算処理手段と、

前記第 2 の演算処理手段において減算／加算されたバイトデータをデジタルデータに変換し、変換されたデジタルデータに対して、前記データ圧縮規格に基づいてデータ解凍処理を施すデータ解凍手段と、

を備えたことを特徴とするモデム装置。

【請求項 1 1】 前記第 1 および第 2 の演算処理手段は、所定のデータパタ

ーンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 1 0 に記載のモデム装置。

【請求項 1 2】 さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、

前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、

を備えたことを特徴とする請求項 1 0 または 1 1 に記載のモデム装置。

【請求項 1 3】 データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、

前記データ送信装置が、

送信するデータを順次読み込み、読み込まれたデータが所定の数値のデジタルデータを含んでいるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第 1 の演算処理手段と、

前記第 1 の演算処理手段によって演算処理されたデータを送信する送信手段と

を備え、

前記データ受信装置が、

前記データ送信装置によって送信されたデータを受信する受信手段と、

前記受信手段によって受信されたデータを順次読み込み、読み込まれたデータが前記所定の数値のデジタルデータを含んでいるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって、前記データが所定の数値のデジタルデータ

を含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、

を備えたことを特徴とするデータ通信システム。

【請求項 1 4】 データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、

前記データ送信装置が、

シリアル入力されたバイナリデータである送信データをバイトデータに変換して一時的に保持する第 1 の保持手段と、

前記第 1 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、

前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理手段と、

前記第 1 の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信する送信手段と、

を備え、

前記データ受信装置が、

シリアル入力されたバイナリデータである受信データをバイトデータに変換して一時的に保持する第 2 の保持手段と、

前記第 2 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、

前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、

前記第 2 の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換する変換してシリアル出力する出力手段と、

を備えたことを特徴とするデータ送信システム。

【請求項 1 5】 前記データ送信装置と前記データ受信装置は、インターネットなどのネットワークによって互いに接続されていることを特徴とする請求項 1 3 または 1 4 に記載のデータ通信システム。

【請求項 1 6】 前記第 1 および第 2 の演算処理手段は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 1 3 ～ 1 5 のいずれか一つに記載のデータ通信システム。

【請求項 1 7】 さらに、前記データ送信装置および前記データ受信装置が、
前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、
前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを、前記データ送信装置と前記データ受信装置とを同期させて変更する情報変更手段と、
を備えたことを特徴とする請求項 1 3 ～ 1 6 のいずれか一つに記載のデータ通信システム。

【請求項 1 8】 連続するデジタルデータを順次読み込む読込工程と、
前記読込工程によって読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理工程と、
前記判定処理工程によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、
を含んだことを特徴とするデータ防護処理方法。

【請求項 1 9】 シリアル入力されたバイナリデータをバイトデータに変換して順次読み込む読込工程と、
前記読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、
前記判定処理工程によって判定された結果、前記所定のバイトコードであると

判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、

前記演算処理工程によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項 2 0】 シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持工程と、

前記保持工程によって保持された所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理工程と、

前記データ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、

前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、

前記演算処理工程によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理工程と、

前記データフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項 2 1】 前記演算処理工程は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 1 8 ～ 2 0 のいずれか一つに記載のデータ防護処理方法。

【請求項 2 2】 連続するデジタルデータである送信データ／受信データを順次読み込む読込工程と、

前記読込工程によって読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第 1 の判定処理工程と、

前記第 1 の判定処理工程によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第 1 の演算処理工程と、

連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第 2 の判定処理工程と、

前記第 2 の判定処理工程によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項 2 3】 シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して順次読み込む第 1 の読込工程と、

前記第 1 の読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理工程と、

前記第 1 の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理工程と、

前記第 1 の演算処理工程によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第 1 の出力工程と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して順次読み込む第 2 の読込工程と、

前記第 2 の読込工程によって読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理工程と、

前記第 2 の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理工程と、

前記第 2 の演算処理工程において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第 2 の出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項 2 4】 シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第 1 の保持工程と、

前記第 1 の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第 1 のデータ抽出処理工程と、

前記第 1 のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理工程と、

前記第 1 の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理工程と、

前記第 1 の演算処理工程によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第 1 のデータフレーム再構成処理工程と、

前記第 1 のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第 1 の出力工程と、

シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第 2 の保持工程と、

前記第 2 の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第 2 のデータ抽出処理工程と、

前記第 2 のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理工程と、

前記第 2 の判定処理工程によって判定された結果、前記所定のバイトコードで

あると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理工程と

前記第 2 の演算処理工程において減算／加算されたバイトデータをもちいてデータフレームを再構成する第 2 のデータフレーム再構成処理工程と、

前記第 2 のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第 2 の出力工程と、

を含んだことを特徴とするデータ防護処理方法。

【請求項 2 5】 前記第 1 および第 2 の演算処理工程は、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする請求項 2 2 ～ 2 4 のいずれか一つに記載のデータ防護処理方法。

【請求項 2 6】 さらに、前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更工程を含んだことを特徴とする請求項 1 8 ～ 2 5 のいずれか一つに記載のデータ防護処理方法。

【請求項 2 7】 前記請求項 1 8 ～ 2 6 のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は、社内 LAN を管理するシステム管理者が、その LAN に属しかつインターネット上で公開されたサーバにアクセスする際に、アクセス時および通信確立後の送受信データを、システム管理者が使用するクライアントとサーバとの間のみで符号化／復号化することによって、システム管理者のみに与えられたアクセス権限を保護することが可能なデータ防護処理装置、モデム装置、データ通信システム、データ防護処理方法、その方法をコンピュータに実行させるプロ

グラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】

インターネットは、オープンなネットワークであるがゆえに、自分が送信したデータが第三者に盗み見される可能性が大きいという問題を有している。そこで、インターネットの一般的な通信形態であるWWW (World Wide Web) サーバとWWWブラウザとの間の通信においては、クレジット・カード番号などの保安性の要するデータを安全に送信したり、メールの送信者や内容が偽造されたりしていないことを証明するために、暗号化技術が導入されている。

【0003】

この暗号化技術の代表的なものとしては、共通鍵暗号法と公開鍵暗号法が知られている。共通鍵暗号法とは、自分と相手が同じ暗号鍵を使って暗号化と復号化をおこなう方法である。一方、公開鍵暗号法は、現在主流となっている暗号方法である。秘密鍵と公開鍵という二つの鍵ペアをもちいて暗号化と復号化をおこない、どちらか一方の鍵で暗号化したデータは、もう一方の鍵を使わないと復号化できないという特徴を有している。

【0004】

この公開鍵暗号法において、秘密鍵は、所持者（使用権限のある者）だけが自由に使うことができるため、自身で安全に管理する必要がある。一方、公開鍵は、WWW上で広く公開されており、誰でも取得して利用することができる。すなわち、秘密鍵を使ってデータを暗号化し、そのデータをペアとなる公開鍵で復号化することで、確かにそのデータが秘密鍵保持者によって暗号化されたことを確認できるという有効な利用が可能になる。この公開鍵暗号法の性質を活用したのが、いわゆる電子署名である。

【0005】

また、WWWサーバとWWWブラウザとの間における代表的な暗号化方式としては、SSL (Secure Socket Layer) が知られている。このSSLは、上記した共通鍵暗号法と公開鍵暗号法とを組み合わせ、両暗号法の利点を生かしたものである。

【0006】

特に、社内LAN (Local Area Network) 等の社内ネットワークでは、専用線等の新たな通信インフラを整備するためのコストが不要になることから、公衆回線と上記した暗号化技術とを利用した、いわゆるVPN (Virtual Private Network) を構築した例が数多くある。

【0007】

また、社内LANでは、さらなるデータの保安性を図るために、ファイアウォールとして、社内クライアントのインターネット・アクセスを代行するプロキシサービスを導入している場合が多い。プロキシサービスは、社内ネットワークに配置されたプロキシサーバが、社内クライアントからのアクセス要求を受け取ると、それを解釈してインターネット上に存在する目的のサーバにアクセスし、結果を受け取って社内クライアントに渡す仕組みである。

【0008】

この仕組みによって、インターネットからはプロキシサーバだけが見え、社内のマシンはまったく見えない。一方、社内クライアントが直接通信する相手はプロキシサーバだけであり、インターネット上のサーバと直接通信することはない。これによって、社内LANにおいて、外部に対するデータの機密化が図られる。なお、ルータやゲートウェイが、プロキシサーバの機能を有している場合も多い。

【0009】

一方、社内LAN等のシステム管理者は、社内LANに直接に接続されたクライアントからではなく、社外から社内LANにアクセスし、サーバを管理することがある。社外からの社内LANへのアクセスは、一般に、公衆回線を介しておこなわれるが、社内LAN内に設置されたアクセスサーバにアクセスする方法（以下、直接アクセス方法と称する。）と、インターネット・サービス・プロバイダのアクセスサーバに接続した後にインターネット経由で社内LANのWWWサーバ等にアクセスする方法（以下、インターネットアクセス方法と称する。）とが知られている。

【0010】

直接アクセス方法では、まず、システム管理者が、ノートパソコン等のクライアント・マシンをもちい、公衆回線を介して社内LANのアクセスサーバに対してダイヤルアップ接続をおこなう。アクセスサーバは、社内LANのメインサーバに接続されている。システム管理者は、このアクセスサーバを経由して、社内LAN内の各種サーバにアクセスすることが可能になる。ここで、各種サーバとしては、コミュニケーションサーバはもちろんのこと、DNS (Domain Name System) サーバ、メールサーバ、WWWサーバ等のインターネット標準プロトコルにしたがったサービスを楽しむためのサーバである。

【0011】

また、インターネットアクセス方法では、まず、システム管理者が、ノートパソコン等のクライアント・マシンをもちい、公衆回線を介してインターネット・サービス・プロバイダのアクセスサーバに対してダイヤルアップ接続をおこなう。インターネット・サービス・プロバイダのアクセスサーバは、ルータを介してインターネットのバックボーンに接続されている。このため、システム管理者は、このアクセスサーバを経由して、インターネットに接続することが可能になる。

【0012】

インターネットに接続された後は、社内LANの各種サーバのうち、バリア・セグメントに位置するサーバ、すなわちインターネット上に公開されたWWWサーバ等のサーバにアクセスする。この際、システム管理者は、たとえばWWWサーバ内の特別なWWWページにアクセスしたり、WWWサーバにアクセスした際に最初に表示されるホームページ上で特別なコマンドを入力することによって、WWWサーバが保持する各種ファイルを管理することができる。

【0013】

【発明が解決しようとする課題】

しかしながら、上記したVPNでは、社外から、公衆回線を介して社内LANにアクセスする際およびアクセス後の送受信において、通信データのすべてに暗号化／復号化処理を施す必要がある。クライアントおよびサーバにおいて、それら処理による負荷の増大は無視できるものではない。特に、保安性を高めようと

すると、暗号化／復号化に要する演算が複雑になる。このため、より高速処理が可能なクライアントおよびサーバを選定する必要がある。これは、VPNの構築にあたってコスト増を意味する。

【0014】

また、暗号化されたデータは、暗号化前のデータと比較してサイズが大きくなってしまうため、電子メールのように比較的サイズの小さなデータの送受信は問題とならない。しかし、大きなサイズのファイルを送受信する場合には、暗号化／復号化処理に時間を多く費やしてしまう。これは、暗号化／復号化処理が、送受信の対象となるデータ全体をすべて受け取った後で、そのデータ全体に対して一度に施される処理であることに起因する。このようなVPNの問題は、システム管理者が社内LANにアクセスする場合も例外ではない。

【0015】

また、上記した直接アクセス方法では、社内LANのアクセスサーバにアクセスした際に、一般にID番号とパスワードの入力が要求され、権限なき者のアクセスは拒絶される。しかし、アクセスサーバのダイヤル番号が知られている場合には、システム管理者以外であっても、そのようなID番号とパスワードの入力を求める状態に移行させることができる。これは、ID番号とパスワードを知らなくても、適当に入力した番号やアルファベットが上記したID番号とパスワードに一致する可能性を否定できない。

【0016】

特に、クラッカー等の悪質な侵入者は、番号やアルファベットのあらゆる組み合わせを自動生成かつ自動入力するツールをもちいて、上記したID番号とパスワードとによる認証を解除しようとする。したがって、従来の直接アクセス方法では、上記したツールをもちいることで、システム管理者のなりすましが可能になってしまう。システム管理者は、一般に、企業の機密データを含めたほとんどすべてのデータを入手する権限が与えられている。このため、システム管理者のなりすましに対しては、これらデータが外部に漏洩することを防ぐことはできない。

【0017】

一方、上記したインターネットアクセス方法においても、ID番号とパスワードの入力要求は直接アクセス方法の場合と共通であり、システム管理者のなりすましを完全に防ぐことは困難である。特に、社内のバリア・セグメント上のサーバは、インターネットの公開性の高さから、制限なくアクセスされることを前提にしている。したがって、システム管理用の特別なWWWページやシステム管理モードに移行するための方法が知られてしまう可能性は高い。これは、システム管理用のID番号やパスワードの入力要求状態へと辿りついてしまうことを意味し、結局は、システム管理者のなりすましの問題へとつながる。

【 0 0 1 8 】

さらに、以上に説明した従来のVPN、直接アクセス方法およびインターネットアクセス方法は、いずれもアプリケーション層レベルにおいて、データ保安を実現しようとするものである。これは、特別な機器を必要とせずとも、コンピュータ・プログラムの知識を有していれば、比較的容易に、データ保安の打破が可能となることを意味する。すなわち、従来のデータ保安技術では、コスト的にも時間的にも、不正侵入者が有利な立場にある。

【 0 0 1 9 】

この発明は、上記に鑑みてなされたものであって、システム管理者が、社内LANのサーバにアクセスする場合に、送受信データを、そのデータ・サイズを増大させることなく、システム管理者のみに与えられたアクセス権限を保護することを可能にしたデータ防護処理装置、モデム装置、データ防護処理方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【 0 0 2 0 】

【課題を解決するための手段】

上記の目的を達成するために、請求項1に記載の発明にかかるデータ防護処理装置にあっては、連続するデジタルデータを順次読み込み、読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理手段と、

前記判定処理手段によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部

または一部に対して、所定の演算値を加算または減算する演算処理手段と、を備えたことを特徴とする。

【 0 0 2 1 】

また、請求項 2 に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータをバイトデータに変換して一時的に保持する保持手段と、前記保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、前記演算処理手段によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【 0 0 2 2 】

また、請求項 3 に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持手段と、前記保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理手段と、前記データ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理手段と、前記判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理手段と、前記演算処理手段によって演算されたバイトデータを持ちいて前記所定のデータフレームを再構成するデータフレーム再構成処理手段と、前記データフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【 0 0 2 3 】

また、請求項 4 に記載の発明にかかるデータ防護処理装置は、請求項 1 ～ 3 の

いずれか一つに記載の発明において、前記演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 2 4 】

また、請求項 5 に記載の発明にかかるデータ防護処理装置は、連続するデジタルデータである送信データ／受信データを順次読み込み、読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第 1 の判定処理手段と、前記第 1 の判定処理手段によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第 1 の演算処理手段と、連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第 2 の判定処理手段と、前記第 2 の判定処理手段によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、を備えたことを特徴とする。

【 0 0 2 5 】

また、請求項 6 に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して一時的に保持する第 1 の保持手段と、前記第 1 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第 1 の演算処理手段と、前記第 1 の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第 1 の出力手段と、シリアル入力されたバイナリデータである受信データ／送

信データをバイトデータに変換して一時的に保持する第2の保持手段と、前記第2の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第2の判定処理手段と、前記第2の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第2の演算処理手段と、前記第2の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第2の出力手段と、を備えたことを特徴とする。

【0026】

また、請求項7に記載の発明にかかるデータ防護処理装置は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第1の保持手段と、前記第1の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第1のデータ抽出処理手段と、

前記第1のデータ抽出処理手段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第1の判定処理手段と、前記第1の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第1の演算処理手段と、前記第1の演算処理手段によって加算されたバイトデータをもちいて前記所定のデータフレームを再構成する第1のデータフレーム再構成処理手段と、前記第1のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第1の出力手段と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第2の保持手段と、前記第2の保持手段から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第2のデータ抽出処理手段と、前記第2のデータ抽出処理手

段から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第2の判定処理手段と、前記第2の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第2の演算処理手段と、前記第2の演算処理手段において減算／加算されたバイトデータを持ちいてデータフレームを再構成する第2のデータフレーム再構成処理手段と、前記第2のデータフレーム再構成処理手段によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第2の出力手段と、を備えたことを特徴とする。

【 0 0 2 7 】

また、請求項8に記載の発明にかかるデータ防護処理装置は、請求項5～7のいずれか一つに記載の発明において、前記第1および第2の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 2 8 】

また、請求項9に記載の発明にかかるデータ防護処理装置は、請求項1～8のいずれか一つに記載の発明において、さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、を備えたことを特徴とする。

【 0 0 2 9 】

また、請求項10に記載の発明にかかるモデム装置は、送信するデジタルデータに対して、標準化されたデータ圧縮規格に基づいてデータ圧縮処理を施すデータ圧縮手段と、前記データ圧縮手段によってデータ圧縮処理を施されたデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み

込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理手段と、前記第 1 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して所定の演算値を加算／減算する第 1 の演算処理手段と、前記第 1 の演算処理手段において加算／減算されたバイトデータを出力する第 1 の出力手段と、受信したデジタルデータをバイトデータに変換し、変換されたバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して前記所定の演算値を減算／加算する第 2 の演算処理手段と、前記第 2 の演算処理手段において減算／加算されたバイトデータをデジタルデータに変換し、変換されたデジタルデータに対して、前記データ圧縮規格に基づいてデータ解凍処理を施すデータ解凍手段と、を備えたことを特徴とする。

【 0 0 3 0 】

また、請求項 1 1 に記載の発明にかかるモデム装置は、請求項 1 0 に記載の発明において、前記第 1 および第 2 の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 3 1 】

また、請求項 1 2 に記載の発明にかかるモデム装置は、請求項 1 0 または 1 1 に記載の発明において、さらに、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更手段と、を備えたことを特徴とする。

【 0 0 3 2 】

また、請求項 1 3 に記載の発明にかかるデータ通信システムは、データ送信装

置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、前記データ送信装置が、送信するデータを順次読み込み、読み込まれたデータが所定の数値のデジタルデータを含んでいるか否かを判定する第1の判定処理手段と、前記第1の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第1の演算処理手段と、前記第1の演算処理手段によって演算処理されたデータを送信する送信手段と、を備え、前記データ受信装置が、前記データ送信装置によって送信されたデータを受信する受信手段と、前記受信手段によって受信されたデータを順次読み込み、読み込まれたデータが前記所定の数値のデジタルデータを含んでいるか否かを判定する第2の判定処理手段と、前記第2の判定処理手段によって、前記データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第2の演算処理手段と、を備えたことを特徴とする。

【 0 0 3 3 】

また、請求項14に記載の発明にかかるデータ通信システムは、データ送信装置と、前記データ送信装置によって送信されたデータを受信するデータ受信装置と、から構成されるデータ通信システムにおいて、前記データ送信装置が、シリアル入力されたバイナリデータである送信データをバイトデータに変換して一時的に保持する第1の保持手段と、前記第1の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第1の判定処理手段と、前記第1の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第1の演算処理手段と、前記第1の演算処理手段によって加算／除算されたバイトデータをバイナリデータに変換して送信する送信手段と、を備え、前記データ受信装置が、シリアル入力されたバイナリデータである受信データをバイトデータに変

換して一時的に保持する第 2 の保持手段と、前記第 2 の保持手段からバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理手段と、前記第 2 の判定処理手段によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理手段と、前記第 2 の演算処理手段において減算／加算されたバイトデータをバイナリデータに変換する変換してシリアル出力する出力手段と、を備えたことを特徴とする。

【 0 0 3 4 】

また、請求項 1 5 に記載の発明にかかるデータ通信システムは、請求項 1 3 または 1 4 に記載の発明において、前記データ送信装置と前記データ受信装置が、インターネットなどのネットワークによって互いに接続されていることを特徴とする。

【 0 0 3 5 】

また、請求項 1 6 に記載の発明にかかるデータ通信システムは、請求項 1 3 ～ 1 5 のいずれか一つに記載の発明において、前記第 1 および第 2 の演算処理手段が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 3 6 】

また、請求項 1 7 に記載の発明にかかるデータ通信システムは、請求項 1 3 ～ 1 6 のいずれか一つに記載の発明において、さらに、前記データ送信装置および前記データ受信装置が、前記所定の数値または所定のバイトコードに関する情報と、前記所定数に関する情報と、前記所定の演算値に関する情報と、を記憶する記憶手段と、前記記憶手段によって記憶された前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを、前記データ送信装置と前記データ受信装置とを同期させて変更する情報変更手段と、を備えたことを特徴とする。

【 0 0 3 7 】

また、請求項 18 に記載の発明にかかるデータ防護処理方法は、連続するデジタルデータを順次読み込む読込工程と、前記読込工程によって読み込まれたデジタルデータが所定の連続パターンの数値であるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定の連続パターンの数値であると判定されたデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、を含んだことを特徴とする。

【 0 0 3 8 】

また、請求項 19 に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータをバイトデータに変換して順次読み込む読込工程と、前記読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、前記演算処理工程によって演算されたバイトデータをバイナリデータに変換してシリアル出力する出力工程と、を含んだことを特徴とする。

【 0 0 3 9 】

また、請求項 20 に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する保持工程と、前記保持工程によって保持された所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出するデータ抽出処理工程と、前記データ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する判定処理工程と、前記判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算または減算する演算処理工程と、前記演算処理工程によって演算されたバイトデータをもちいて前記所定のデータフレームを再構成するデータフレーム再構成処理工程と、前記データフレーム再構成処理工程によって再構成された

データフレームをバイナリデータに変換してシリアル出力する出力工程と、を含んだことを特徴とする。

【 0 0 4 0 】

また、請求項 2 1 に記載の発明にかかるデータ防護処理方法は、請求項 1 8 ～ 2 0 のいずれか一つに記載の発明において、前記演算処理工程が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 4 1 】

また、請求項 2 2 に記載の発明にかかるデータ防護処理方法は、連続するデジタルデータである送信データ／受信データを順次読み込む読込工程と、前記読込工程によって読み込まれた送信データ／受信データが所定の数値のデジタルデータを含んでいるか否かを判定する第 1 の判定処理工程と、前記第 1 の判定処理工程によって、前記送信データ／受信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する所定数のデジタルデータの全部または一部に対して、所定の演算値を加算／減算する第 1 の演算処理工程と、連続するデジタルデータである受信データ／送信データを順次読み込み、読み込まれた受信データ／送信データが前記所定の数値のデジタルデータを含んでいるか否かを判定する第 2 の判定処理工程と、前記第 2 の判定処理工程によって、前記受信データ／送信データが所定の数値のデジタルデータを含んでいると判定された場合に、前記所定の数値のデジタルデータの後に連続する前記所定数のデジタルデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理工程と、を含んだことを特徴とする。

【 0 0 4 2 】

また、請求項 2 3 に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換して順次読み込む第 1 の読込工程と、前記第 1 の読込工程によって読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第 1 の判定処理工程と、前記第 1 の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または

一部に対して、所定の演算値を加算／除算する第1の演算処理工程と、前記第1の演算処理工程によって加算／除算されたバイトデータをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第1の出力工程と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換して順次読み込む第2の読込工程と、前記第2の読込工程によって読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第2の判定処理工程と、前記第2の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第2の演算処理工程と、前記第2の演算処理工程において減算／加算されたバイトデータをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第2の出力工程と、を含んだことを特徴とする。

【0043】

また、請求項24に記載の発明にかかるデータ防護処理方法は、シリアル入力されたバイナリデータである送信データ／受信データをバイトデータに変換し、変換されたバイトデータを所定のデータフレームごとに一時的に保持する第1の保持工程と、前記第1の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第1のデータ抽出処理工程と、前記第1のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが所定のバイトコードであるか否かを判定する第1の判定処理工程と、前記第1の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する所定数のバイトデータの全部または一部に対して、所定の演算値を加算／除算する第1の演算処理工程と、前記第1の演算処理工程によって加算されたバイトデータを持ちいて前記所定のデータフレームを再構成する第1のデータフレーム再構成処理工程と、前記第1のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して送信データ／受信データとしてシリアル出力する第1の出力工程と、シリアル入力されたバイナリデータである受信データ／送信データをバイトデータに変換し、変換されたバイトデータを所定

のデータフレームごとに一時的に保持する第 2 の保持工程と、前記第 2 の保持工程から前記所定のデータフレームを構成するバイトデータの一部を処理対象データとして抽出する第 2 のデータ抽出処理工程と、前記第 2 のデータ抽出処理工程から前記処理対象データを構成するバイトデータを順次読み込み、読み込まれたバイトデータが前記所定のバイトコードであるか否かを判定する第 2 の判定処理工程と、前記第 2 の判定処理工程によって判定された結果、前記所定のバイトコードであると判定されたバイトデータの後に連続する前記所定数のバイトデータの全部または一部に対して、前記所定の演算値を減算／加算する第 2 の演算処理工程と、前記第 2 の演算処理工程において減算／加算されたバイトデータをもちいてデータフレームを再構成する第 2 のデータフレーム再構成処理工程と、前記第 2 のデータフレーム再構成処理工程によって再構成されたデータフレームをバイナリデータに変換して受信データ／送信データとしてシリアル出力する第 2 の出力工程と、を含んだことを特徴とする。

【 0 0 4 4 】

また、請求項 2 5 に記載の発明にかかるデータ防護処理方法は、請求項 2 2 ～ 2 4 のいずれか一つに記載の発明において、前記第 1 および第 2 の演算処理工程が、所定のデータパターンまたはバイトパターンの演算値を加算または減算の対象となるデジタルデータまたはバイトデータに順次加算または減算することを特徴とする。

【 0 0 4 5 】

また、請求項 2 6 に記載の発明にかかるデータ防護処理方法は、請求項 1 8 ～ 2 5 のいずれか一つに記載の発明において、さらに、前記所定の数値または所定のバイトコードに関する情報、前記所定数に関する情報、前記所定の演算値に関する情報のうちの少なくとも一つを変更する情報変更工程を含んだことを特徴とする。

【 0 0 4 6 】

また、請求項 2 7 に記載の発明にかかる記録媒体は、請求項 1 8 ～ 2 6 のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、当該プログラムをコンピュータによって読み取ることが可能となり、これ

によって、請求項 9 ～ 1 6 の動作をコンピュータによって実現することが可能である。

【 0 0 4 7 】

【発明の実施の形態】

以下、この発明にかかるデータ防護処理装置、モデム装置およびデータ防護処理方法の好適な実施の形態について添付図面を参照し、詳細に説明する。なお、この実施の形態によってこの発明が限定されるものではない。

【 0 0 4 8 】

（実施の形態 1）

まず、実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法は、シリアル入力されるビットデータ列に対してバイト変換をおこなうことでバイト列を取得する。そして、取得したバイト列に含まれる所定のバイトデータの存在を条件として、バイトコードから所定範囲にわたるバイトデータに対して所定の防護キー値を加算することで符号化をおこなうことを特徴としている。また、逆の手順によって復号化をおこなうことも特徴とする。

【 0 0 4 9 】

図 1 は、実施の形態 1 にかかるデータ防護処理装置の概略構成を示すブロック図である。図 1 に示すデータ防護処理装置 1 0 は、通信回線上や通信機器へと送信しようとする送信データに対して符号化処理を施す符号化処理部と、通信回線上や通信機器から受信した受信データに対して復号化処理を施す復号化処理部と、付加条件／付加範囲／防護キー記憶部 3 0 と、を備えて構成される。

【 0 0 5 0 】

まず、付加条件／付加範囲／防護キー記憶部 3 0 は、付加条件、付加範囲および防護キー値を記憶するものである。ここで、付加条件とは、バイトデータが、どのバイトコードを示した場合にそのバイトデータからいくつ後のバイトデータに対して防護キー値の加算をおこなうかを示すものである。したがって、この付加条件は、所定のバイトコードと加算開始位置を示す数値とから構成される。

【 0 0 5 1 】

また、付加範囲とは、付加条件によって示される加算開始位置から、いくつかのバイトデータにわたって防護キー値を加算するかを示すものであり、その範囲を示す数値によって表わされる。防護キー値とは、上記したように、バイトデータに加算する数値を表わすものである。

【 0 0 5 2 】

また、付加条件／付加範囲／防護キー記憶部 3 0 に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。たとえば、インターネット上の時刻サーバや GPS (Global Positioning System) 衛星の原子時計に同期して、一斉に防護キー値を所定の値に変更するといった形態を採用することができる。これによって、より強固なデータ保安を図ることが可能になる。

【 0 0 5 3 】

また、データの送信側から付加条件、付加範囲および防護キー値に関する情報を取得して、その情報に基づいて、操作者が図示を省略するキーボードなどを持ちいて書き換えることもできる。その際、あらかじめ図示を省略する変換テーブルを備え、数字または記号により書かれたデータを入力することによって、上記変換テーブルで付加条件、付加範囲および防護キー値に関するデータに変換して入力するようにしてもよい。このように送受信者間のみで独自の通信をおこなうことができる。

【 0 0 5 4 】

符号化処理部は、第 1 送信バッファ 2 2 と、防護キー付加位置判定部 2 4 と、防護キー付加処理部 2 6 と、第 2 送信バッファ 2 8 と、から構成される。第 1 送信バッファ 2 2 は、外部から受け取ったデータ、特にシリアルビットデータを、少なくとも複数のバイトが構成できる容量分のデータを蓄積する記憶部である。また、この第 1 送信バッファ 2 2 は、デジタルデータのシリアルーパラレル変換を可能とした FIFO (First In First Out) メモリとしての機能を果たす。

【 0 0 5 5 】

防護キー付加位置判定部 2 4 は、第 1 送信バッファに蓄積されたバイトデータ

をその蓄積順に取り出し、取り出したバイトデータが、上記した付加条件によって示されるバイトコードに一致するか否かを判定するものである。防護キー付加位置判定部24は、第1送信バッファから取り出したバイトデータが上記付加条件を満たす場合には、たとえば、その旨を示す付加フラグをON状態にしたり、後述するように付加カウンタをカウントアップする。

【0056】

防護キー付加処理部26は、第1送信バッファ22から取り出されたバイトデータを、防護キー付加位置判定部24を介して受け取り、受け取ったバイトデータが上記付加条件を満たす場合に、そのバイトデータに上記防護キー値を加算する。具体的には、防護キー付加処理部26は、上記付加フラグや付加カウンタの状態に応じて、バイトデータに対して防護キー値を加算するか否かを判定する。

【0057】

第2送信バッファ28は、防護キー付加処理部26において付加処理が施されたバイトデータおよび付加処理が施されなかったバイトデータを蓄積する記憶部である。また、この第2送信バッファ28は、デジタルデータのパラレル-シリアル変換を可能としたFIFOメモリとしての機能を果たす。したがって、符号化処理部は、第1送信バッファ22が受け取ったデータに対し、所定の条件を満たすデータ部のみを変容させることになる。特に、その変容前後において、データサイズに変化がないことを特徴としている。

【0058】

一方、復号化処理部は、第1受信バッファ38と、防護キー除去位置判定部36と、防護キー除去処理部34と、第2受信バッファ32と、から構成され、上述した符号化処理部と逆の処理をおこなう。第1受信バッファ38は、上記した第1送信バッファと同様の機能を果たす記憶部である。

【0059】

防護キー除去位置判定部36は、第1受信バッファに蓄積されたバイトデータをその蓄積順に取り出し、取り出したバイトデータが、上記した付加条件によって示されるバイトコードに一致するか否かを判定するものである。防護キー除去

位置判定部 3 6 は、第 1 受信バッファから取り出したバイトデータが上記付加条件を満たす場合には、たとえば、その旨を示す付加フラグを ON 状態にしたり、後述するように付加カウンタをカウントアップする。したがって、この防護キー除去位置判定部 3 6 は、機能としては上記した防護キー付加位置判定部 2 4 と同じであり、復号化処理部において防護キー除去位置判定部 3 6 を設けずに、防護キー付加位置判定部 2 4 を兼用してもよい。

【 0 0 6 0 】

防護キー除去処理部 3 4 は、第 1 受信バッファ 3 8 から取り出されたバイトデータを、防護キー除去位置判定部 3 6 を介して受け取り、受け取ったバイトデータが上記付加条件を満たす場合に、そのバイトデータから上記防護キー値を差し引く。具体的には、防護キー除去処理部 3 4 は、上記付加フラグや付加カウンタの状態に応じて、バイトデータに対して防護キー値を差し引くか否かを判定する。

【 0 0 6 1 】

第 2 受信バッファ 3 2 は、防護キー除去処理部 3 4 において除去処理が施されたバイトデータおよび除去処理が施されなかったバイトデータを蓄積する記憶部である。また、この第 2 受信バッファ 3 2 は、デジタルデータのパラレルーシリアル変換を可能とした F I F O メモリとしての機能を果たす。したがって、復号化処理部は、第 1 受信バッファ 3 8 が受け取ったデータに対し、所定の条件を満たすデータ部のみを変容させることになる。特に、上記した符号化処理部によって変容されたデータに対しては復号化処理を施すことになる。

【 0 0 6 2 】

したがって、データ防護処理装置 1 0 から出力された送信データは、データ防護処理装置 1 0 をもちいて受信しなければ、送信内容を正しく取得することはできない。すなわち、データ防護処理装置 1 0 は、符号化／復号化処理を、付加条件／付加範囲／防護キー記憶部 3 0 に記憶された内容にしたがってデータサイズを増減させることなく実行する装置である。

【 0 0 6 3 】

つぎに、このデータ防護処理装置 1 0 の動作について、符号化処理および復号

化処理に分けて説明する。ここでは、説明を簡単にするために、上記した付加条件のうち加算開始位置を1とする。これは、付加条件によって示されるバイトコード、すなわち付加処理を実行するきっかけとなるバイトデータのつぎに位置するバイトデータから防護キー値の加算または減算をおこなうことを意味する。

【0064】

まず、データ防護処理装置10の符号化処理について説明する。図2は、実施の形態1にかかるデータ防護処理装置の符号化処理を示すフローチャートである。データ防護処理装置10は、符号化処理を開始するにあたって、まず、符号化の対象となる送信データを第1送信バッファ22に取りこむ。そして、防護キー付加位置判定部24が、第1送信バッファ22から1バイト分のデータを読み出す（ステップS201）。また、防護キー付加位置判定部24は、自身が管理する付加カウンタが0より大きい値を示しているか否かを判定する（ステップS202）。

【0065】

ステップS202において付加カウンタが0である場合には、防護キー付加位置判定部24は、第1送信バッファ22から読み出したバイトデータに対して付加処理を施す必要はないと判断し、現在読み出しているバイトデータが防護キー付加条件、すなわち上記したバイトコードと一致するか否かを判定する（ステップS207）。

【0066】

ステップS207においてバイトデータが防護キー付加条件と一致しない場合には、防護キー付加位置判定部24は、現在読み出しているバイトデータをそのまま次段の防護キー付加処理部26に渡し、防護キー付加処理部26は付加処理を実行することなく、そのバイトデータを第2送信バッファ28に書き込む（ステップS209）。

【0067】

ステップS207においてバイトデータが防護キー付加条件と一致する場合には、防護キー付加位置判定部24は、上記した付加カウンタを1にセットし（ステップS208）、ステップS209の処理をおこなう。

【 0 0 6 8 】

ステップ S 2 0 2 において付加カウンタが 0 より大きい場合には、防護キー付加位置判定部 2 4 は、第 1 送信バッファ 2 2 から読み出したバイトデータに対して付加処理を施す必要があると判断し、次段の防護キー付加処理部 2 6 に、現在読み出しているバイトデータを渡すとともに、付加処理を依頼する。これによって、防護キー付加処理部 2 6 は、受け取ったバイトデータに、付加条件／付加範囲／防護キー記憶部 3 0 に記憶されている防護キー値を加算する（ステップ S 2 0 3）。

【 0 0 6 9 】

図 3 は、防護キー値の加算処理を説明するための説明図である。ステップ S 2 0 3 における加算処理は、たとえば、図 3 に示すように、防護キー値がヘキサコード“1 E”で表わされ、第 1 送信バッファ 2 2 から読み出したデータがバイナリコードで“1 0 1 1 0 0 1 0”と表わされたバイトデータ、すなわちヘキサコード“B 2”で表わされる場合、バイトデータ“B 2”に防護キー値“1 E”を加算することによりおこなう。したがって、この場合、加算結果として、バイナリコード“1 1 0 1 0 0 0 0”と表わされたバイトデータ、すなわちヘキサコード“D 0”を得ることができる。

【 0 0 7 0 】

防護キー付加位置判定部 2 4 は、防護キー付加処理部 2 6 による加算処理が終わると、または防護キー付加処理部 2 6 に対して加算処理を依頼すると、付加カウンタが付加条件／付加範囲／防護キー記憶部 3 0 に記憶されている付加範囲を超えているか否かを判定する（ステップ S 2 0 4）。

【 0 0 7 1 】

ステップ S 2 0 4 において付加カウンタが付加範囲を超えていない場合は、防護キー付加位置判定部 2 4 は、付加カウンタの値をインクリメントし（ステップ S 2 0 6）、ステップ S 2 0 9 の処理をおこなう。一方、ステップ S 2 0 4 において付加カウンタが付加範囲を超えている場合は、防護キー付加位置判定部 2 4 は、付加カウンタの値をリセットし（ステップ S 2 0 5）、ステップ S 2 0 9 の処理をおこなう。

【 0 0 7 2 】

以上の処理によって、データ防護処理装置 1 0 は、第 1 送信バッファ 2 2 に蓄積されたバイトデータに対し、付加条件／付加範囲／防護キー記憶部 3 0 に記憶された諸条件にしたがった符号化を実現する。図 4 は、符号化処理によって得られるバイトデータ列の例を示す図である。

【 0 0 7 3 】

図 4 に示すように、付加条件がバイトコード“5 D”のつぎからとし、防護キー値を“1 E”、付加範囲を 3 とした場合には、データ防護処理装置 1 0 の符号化処理によって、“5 D 9 B 1 1 4 0 A 9”の部分は、“5 D B 9 2 F 5 E A 9”に変容され、“5 D 8 8 F A 1 B 3 3”の部分は、“5 D A 6 1 9 3 9 3 3”に変容される。ここで、“F A”から“1 9”に変容されているように、防護キー値を加算した結果が、1 バイトで表わされる数値範囲を超える場合には、その超えた部分の数値を加算結果とする。

【 0 0 7 4 】

また、上記の例においては、防護キー値を一種類のみ設定していたが、防護キー値を複数の値から構成されるデータパターンとして用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算するようにしてもよい。たとえば、図 4 に示した例で、付加条件および付加範囲は同じで、防護キー値を“1 E, A B, 7 F”とすると、“5 D”のつぎの“9 B”に対して、“1 E”を加算され、つぎの“1 1”に対して“A B”を加算し、つぎの“4 0”に対して“7 F”を加算する。

【 0 0 7 5 】

また、付加条件、付加範囲の設定方法については、以下のような方法であってもよい。たとえば、付加条件を“5 D”つぎとそのつぎをとばして 3 つ先からとし、付加範囲を一つおきに 3 バイトとする。それによって、図 4 に示した例をもちいると、加算の対象となるのは、（“9 B”と“1 1”をとばした 3 つ先の）“4 0”と“D D”と“3 8”ということになる。いずれにせよ、所定の数値のバイトデータの後に連続する所定数のバイトデータの全部または一部であれば、その内容についてはどのようなものであってもよい。

【0076】

プログラムは、基本的には8ビットコードの配列として表現されており、そのソースでコマンド等を構成するアルファベットや数値を表わすのに、8ビットコードのうち7ビットしかもちいておらず、最上位ビットである8ビット目を“1”に置換すると、コンピュータ上で認識できないコードになる。したがって、対象のデータがプログラムである場合は、防護キー値として、8ビット目を“1”に置換するようなヘキサコードとして、“80”～“FF”のいずれかをもちいるとより有効である。

【0077】

つぎに、データ防護処理装置10の復号化处理について説明する。図5は、実施の形態1にかかるデータ防護処理装置の復号化处理を示すフローチャートである。データ防護処理装置10は、復号化处理を開始するにあたって、まず、復号化の対象となる受信データを第1受信バッファ38に取りこむ。そして、防護キー除去位置判定部36が、第1受信バッファ38から1バイト分のデータを読み出す（ステップS501）。また、防護キー除去位置判定部36は、自身が管理する付加カウンタが0より大きい値を示しているか否かを判定する（ステップS502）。

【0078】

ステップS502において付加カウンタが0である場合には、防護キー除去位置判定部36は、第1受信バッファ38から読み出したバイトデータに対して除去処理を施す必要はないと判断し、現在読み出しているバイトデータが防護キー付加条件、すなわち上記したバイトコードと一致するか否かを判定する（ステップS507）。

【0079】

ステップS507においてバイトデータが防護キー付加条件と一致しない場合には、防護キー除去位置判定部36は、現在読み出しているバイトデータをそのまま次段の防護キー除去処理部34に渡す。そして、防護キー除去処理部34は除去処理を実行することなく、そのバイトデータを第2受信バッファ32に書き込む（ステップS509）。

【0080】

ステップS507においてバイトデータが防護キー付加条件と一致する場合には、防護キー除去位置判定部36は、上記した付加カウンタを1にセットし（ステップS508）、ステップS509の処理をおこなう。

【0081】

ステップS502において付加カウンタが0より大きい場合には、防護キー除去位置判定部36は、第1受信バッファ38から読み出したバイトデータに対して減算処理を施す必要があると判断し、次段の防護キー除去処理部34に、現在読み出しているバイトデータを渡すとともに、減算処理を依頼する。これによって、防護キー除去処理部34は、受け取ったバイトデータから、付加条件／付加範囲／防護キー記憶部30に記憶されている防護キー値を差し引く（ステップS503）。なお、この減算処理は、図3に示した加算処理と逆の処理であるので、ここではその説明を省略する。

【0082】

防護キー除去位置判定部36は、防護キー除去処理部34による減算処理が終わると、または防護キー除去処理部34に対して減算処理を依頼すると、付加カウンタが付加条件／付加範囲／防護キー記憶部30に記憶されている付加範囲を超えているか否かを判定する（ステップS504）。

【0083】

ステップS504において付加カウンタが付加範囲を超えていない場合は、防護キー除去位置判定部36は、付加カウンタの値をインクリメントし（ステップS506）、ステップS509の処理をおこなう。一方、ステップS504において付加カウンタが付加範囲を超えている場合は、防護キー除去位置判定部36は、付加カウンタの値をリセットし（ステップS505）、ステップS509の処理をおこなう。

【0084】

以上の処理によって、データ防護処理装置10は、第1受信バッファ38に蓄積されたバイトデータに対し、付加条件／付加範囲／防護キー記憶部30に記憶された諸条件にしたがった復号化を実現する。

【 0 0 8 5 】

以上に説明したように、実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法によれば、通信回線上や通信機器に送信しようとするシリアルデータをバイトごとに監視して、そのバイトデータが所定のバイトコードに一致しているか否かを判定し、一致している場合には、その一致箇所から所定の個数後に受け取ったバイトデータを開始位置として、その開始位置にあるバイトデータから所定の個数にわたるバイトデータに所定の値を加算することで符号化を実現しているので、データの符号化をデータサイズの変化なく実現することができる。

【 0 0 8 6 】

また、通信回線上や通信機器から受信したシリアルデータをバイトごとに監視して、そのバイトデータが所定のバイトコードに一致しているか否かを判定し、一致している場合には、その一致箇所から所定の個数後に受け取ったバイトデータを開始位置として、その開始位置にあるバイトデータから所定の個数にわたるバイトデータから所定の値を差し引くことで、上記した符号化に対応した復号化を実現することができる。

【 0 0 8 7 】

したがって、実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法は、送受信する一連のデジタルコンテンツのデジタルデータのすべてを受け取らずとも、実際に受け取った部分から順に符号化／復号化処理を実行することが可能になるので、送信／受信バッファとして大容量のものを必要とすることなく、装置構成を安価にすることができる。

【 0 0 8 8 】

特に、このデータ防護処理装置を互いに有する二者間においては、データの機密化と高速な送受信をともに実現することができる。

【 0 0 8 9 】

なお、以上に説明した実施の形態 1 では、符号化処理において防護キー値を加算し、復号化処理において防護キー値を減算するとしたが、逆に、符号化処理において防護キー値を減算し、復号化処理において防護キー値を加算してもよい。

【 0 0 9 0 】

また、以上に説明した実施の形態 1 にかかるデータ防護処理装置において、付加条件／付加範囲／防護キー記憶部 3 0 に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【 0 0 9 1 】

(実施の形態 2)

つぎに、実施の形態 2 にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態 2 は、実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法を、上述した直接アクセス方法に適用した例を説明するものである。したがって、実施の形態 1 において説明した内容については同様であるのでその説明は省略する。

【 0 0 9 2 】

図 6 は、実施の形態 2 にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。図 6 においては、システム管理者の使用するクライアント 1 3 0 が公衆回線 1 4 0 を介して社内 LAN 1 2 0 のアクセスサーバ 1 2 4 に接続する場合を示している。

【 0 0 9 3 】

図 6 において、社内 LAN 1 2 0 は、専用線を介してインターネット・サービス・プロバイダ 1 1 0 に接続されており、インターネット・サービス・プロバイダ 1 1 0 は、ルータ R 1 0 をインターネット 1 0 0 のバックボーンに接続している。これによって、社内 LAN 1 2 0 内のクライアント 1 2 8 は、ルータ R 2 0 を介して、インターネット 1 0 0 に接続することが可能となっている。

【 0 0 9 4 】

図 6 において、直接アクセス方法に実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法を適用するには、クライアント 1 3 0 側の TA (ターミナルアダプタ) / モデムと、アクセスサーバ 1 2 4 側の TA (ターミナルアダプタ) / モデムとに、それぞれ実施の形態 1 において説明したデータ防護処理方法を実現する機能を設ける。

【 0 0 9 5 】

クライアント 1 3 0 が社内 LAN のアクセスサーバ 1 2 4 に接続する場合を考える。まず、クライアント 1 3 0 は、アクセスサーバ 1 2 4 にダイヤルすることでダイヤルアップ接続を確立する。

【 0 0 9 6 】

つづいてアクセスサーバ 1 2 4 は、ID 番号 / パスワード入力要求を示した送信データをデータ防護機能付 TA / モデム 1 2 6 に出力する。そこで、送信データは、実施の形態 1 に説明した符号化処理を施されるとともに、公衆回線 1 4 0 の信号規格に応じて、アナログ変換や電圧変換の処理を施される。

【 0 0 9 7 】

これによって、符号化された送信データは、公衆回線 1 4 0 を介してデータ防護機能付 TA / モデム 1 3 2 に到達し、そこで実施の形態 1 に説明した復号化処理が施される。復号化された送信データは、クライアント 1 3 0 において解釈され、その表示装置上に ID 番号 / パスワード入力要求画面として表示される。

【 0 0 9 8 】

システム管理者は、ID 番号 / パスワード入力要求に対して、ID 番号とパスワードを入力し、クライアント 1 3 0 は、入力された ID 番号とパスワードを送信データとして、データ防護機能付 TA / モデム 1 3 2 に出力する。そこで、送信データは、実施の形態 1 に説明した符号化処理を施されるとともに、公衆回線 1 4 0 の信号規格に応じて、アナログ変換や電圧変換の処理を施される。

【 0 0 9 9 】

これによって、符号化された送信データは、公衆回線 1 4 0 を介してデータ防護機能付 TA / モデム 1 2 6 に到達し、そこで実施の形態 1 に説明した復号化処理が施される。復号化された送信データは、アクセスサーバ 1 2 4 において解釈され、アクセスが正規のシステム管理者によるものである否かの認証確認がおこなわれる。

【 0 1 0 0 】

アクセスサーバ 1 2 4 において正規のシステム管理者であることが認証されると、アクセスサーバ 1 2 4 は、クライアント 1 3 0 を、社内 LAN 1 2 0 内の WWW ・ DNS ・ メールサーバ 1 2 2 に接続する。これによって、クライアント 1

30は、社内LAN120内のWWW・DNS・メールサーバ122にアクセスすることが可能となり、システム管理者の権限によるシステム管理およびファイル管理をおこなうことができる。

【0101】

ただし、クライアント130とWWW・DNS・メールサーバ122と間のデータ送受信においても、データ防護機能付TA/モデム132および126を経由するため、これらのシステム管理およびファイル管理をおこなうに際して入力されるコマンドや送受信されるファイルに対しても、実施の形態1において説明した符号化/復号化がおこなわれる。

【0102】

すなわち、社内LAN120に設置されるアクセスサーバ124のTA/モデムに、実施の形態1で説明したデータ防護機能が付加されている限り、同データ防護機能が付加されたTA/モデムを備えたクライアントを使用しなければ、社外から社内LANのWWW・DNS・メールサーバ122にアクセスすることはできない。

【0103】

特に、データ防護機能が付加されたTA/モデムを備えたクライアントを使用しなければ、アクセスサーバ124が要求するID番号/パスワード入力をも実行することができないため、ID番号/パスワード自動生成ツールを使用することによる「なりすまし」の問題も防げることになる。

【0104】

ここで、公衆回線140としてアナログ回線を使用する場合には、クライアント130側およびアクセスサーバ124側において、ともにモデムを必要とするが、モデムの場合、デジタルデータからアナログデータに変換するに際して、通常、データ圧縮やフレーム化をおこなっている。

【0105】

したがって、モデムにおいては、上記データ防護機能を付加させるタイミングが幾通り存在する。図7は、データ防護機能付きモデムの一例を示すブロック図である。図7において、データ防護機能付きモデムは、従来のモデムにおいて送

信処理部を構成するバッファ 1 5 1、データ圧縮部 1 5 2、フレーム処理部 1 5 3、変調処理部 1 5 4 および D/A コンバータ 1 5 5 と、受信処理部を構成するバッファ 1 6 1、データ解凍部 1 6 2、データ抽出処理部 1 6 3、復調処理部 1 6 4 および A/D コンバータ 1 6 5 と、に加えて、図 1 に示したデータ防護処理装置 1 0 を備えている。

【 0 1 0 6 】

特に、データ防護処理装置 1 0 は、データ送信時に、データ圧縮部 1 5 2 によって圧縮されたデジタルデータに対して符号化処理を施し、符号化されたデータをフレーム処理部 1 5 3 へと受け渡している。また、逆に、データ受信時には、データ抽出処理部 1 6 3 によって抽出されたデジタルデータに対して復号化処理を施し、復号化されたデータをデータ解凍部 1 6 2 へと受け渡している。

【 0 1 0 7 】

これによって、モデムとデータ防護処理装置とを一体化することができるとともに、データ圧縮後のコンパクトなデータに対して符号化をおこなうことから、送信するデジタルコンテンツに対して施す符号化処理を削減することができ、データの機密性をともなった、より高速なデータ送受信が可能となる。

【 0 1 0 8 】

以上に説明したように、実施の形態 2 にかかるデータ防護処理装置およびデータ防護処理方法によれば、社外のクライアント 1 3 0 側と社内のアクセスサーバ 1 2 4 側のそれぞれのモデム/T A に、実施の形態 1 で説明したデータ防護機能を付加することによって、それら二者間のみににおいて正常な通信が可能になるので、アクセスサーバ 1 2 4 が外部との接続を許可する社内のサーバに対しては、データ防護機能を有するクライアントのみがアクセス可能となり、他のクライアントからの不正侵入を防止することができる。

【 0 1 0 9 】

また、以上に説明した実施の形態 2 にかかるデータ防護処理装置においては、一種類だけの防護キー値を設定していたが、複数の値から構成されるデータパターンを用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算してもよい。

【 0 1 1 0 】

また、以上に説明した実施の形態 2 にかかるデータ防護処理装置において、実施の形態 1 において説明したのと同様に、付加条件／付加範囲／防護キー記憶部 3 0 に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【 0 1 1 1 】

(実施の形態 3)

つぎに、実施の形態 3 にかかるデータ防護処理装置およびデータ防護処理方法について説明する。実施の形態 3 は、実施の形態 1 にかかるデータ防護処理装置およびデータ防護処理方法を、上述したインターネットアクセス方法に適用した例を説明するものである。したがって、実施の形態 1 において説明した内容については同様であるのでその説明は省略する。

【 0 1 1 2 】

図 8 は、実施の形態 3 にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。図 8 においては、システム管理者の使用するクライアント 2 5 0 が公衆回線 2 6 0、インターネット・サービス・プロバイダ 2 1 0、インターネット 1 0 0 およびインターネット・サービス・プロバイダ 1 1 0 を介して、社内 LAN 2 2 0 のバリア・セグメントに位置する WWW・DNS・メールサーバ 2 2 2 にアクセスする場合を示している。

【 0 1 1 3 】

図 8 において、社内 LAN 2 2 0 は、専用線を介してインターネット・サービス・プロバイダ 1 1 0 に接続されており、インターネット・サービス・プロバイダ 1 1 0 は、ルータ R 1 0 をインターネット 1 0 0 のバックボーンに接続している。これによって、社外のクライアントは、インターネット 1 0 0、インターネット・サービス・プロバイダ 1 1 0 のルータ R 1 0、社内 LAN 2 2 0 内のルータ R 4 0 を介して、社内 LAN 2 2 0 内のバリア・セグメントに位置する WWW・DNS・メールサーバ 2 2 2 にアクセスすることが可能になっている。

【 0 1 1 4 】

また、社内 LAN 2 2 0 は、ファイアウォールとしてプロキシサーバ 2 4 0 を

備えており、社内のクライアント238は、社内向けのDNS・メールサーバ236と社外向けのWWW・DNS・メールサーバ222との間のデータ送受信、ならびにインターネットとの接続をフィルタリングしている。

【0115】

図8において、インターネットアクセス方法に実施の形態1にかかるデータ防護処理装置およびデータ防護処理方法を適用するには、クライアント250側と、社内LAN220内のWWW・DNS・メールサーバ222側とに、それぞれ実施の形態1において説明したデータ防護処理装置を設ける。

【0116】

この際特に、クライアント250側では、TA/モデム254とクライアント250との間に、WWW・DNS・メールサーバ222側では、LANボード226とWWW・DNS・メールサーバ222との間に、それぞれデータ防護処理装置を配置する必要がある。

【0117】

ここで、インターネットではOSI (Open System Interconnection) 参照モデルのうち、物理層/データリンク層をEthernetとし、トランスポート層/ネットワーク層をTCP/IPとした通信プロトコルが主流であり、これら通信プロトコルに基づいて送受信されるデータ単位、すなわちデータフレーム（またはデータパケット）は、各通信プロトコルに準じたデータをカプセル化して生成されている。

【0118】

たとえば、最下層となるEthernetフレームは、MAC (Media Access Control) アドレス等を含んだEthernetヘッダ部とEthernetデータ部から構成される。そして、Ethernetデータ部は、IPアドレス等を含んだIPヘッダ部とIPデータ部とから構成される。また、IPデータ部は、ポート番号等を含んだTCPヘッダ部とTCPデータ部とから構成される。さらに、TCPデータ部には、アプリケーション層に位置するHTTP (Hypertext Transfer Protocol) やFTP (File Transfer Protocol) 等のヘッダ部とデータ

部から構成される。

【0119】

また、LANやインターネット接続を実現するために必須となるネットワーク機器は、そのレベルに応じて、通信回線上に伝送されているEthernetフレームから、上記した各通信プロトコルのヘッダ部の内容を読み出している。たとえば、スイッチング・ハブは、Ethernetヘッダ部からMACアドレスを抽出して経路制御をおこなっており、ルータは、IPヘッダ部からIPアドレスを抽出して経路制御をおこなっている。さらに、プロキシサーバでは、TCPヘッダ部からポート番号を抽出してフィルタリングをおこなっている。

【0120】

このようにインターネット標準プロトコルに基づいて伝送されるデータフレームは、HTTPアプリケーション層レベルのHTTPやFTPのデータ部に対してのみ変容させる自由度があり、その他のデータフレーム構成部分について不用意に符号化をおこなってしまうと、送信先に到達しないおそれが高くなる。

【0121】

そこで、実施の形態3にかかるデータ防護処理装置およびデータ防護処理方法では、実施の形態1に示したデータ防護処理装置およびデータ防護処理に加え、上記したデータフレームを構成するデータのうち符号化／復号化をおこなうデータ部分を指定する機能を付加している。

【0122】

図9は、実施の形態3にかかるデータ防護処理装置の概略構成を示すブロック図である。なお、図9において、図1と共通する部分については同一符号を付してその説明を省略する。図9に示すデータ防護処理装置20において、図1と異なる点は、符号化処理部にフレームバッファ42、データフレーム抽出処理部44およびデータフレーム置換処理部46が追加され、復号化処理部にフレームバッファ52、データフレーム抽出処理部54およびデータフレーム置換処理部56が追加されたことである。

【0123】

フレームバッファ42は、送信しようとするデータ、特にアプリケーション層

以下の階層に位置するTCPデータやIPデータが含まれた状態のデータフレームを受け取って保持する記憶部である。また、データフレーム抽出処理部44は、フレームバッファ42に保持されたデータフレームから、HTTPデータ等のアプリケーション層に位置するデータを抽出し、抽出したデータを第1送信バッファ22に書き込む処理をおこなう。

【0124】

そして、データフレーム置換処理部46は、フレームバッファ42に保持されたデータフレームのうちデータフレーム抽出処理部44によって抽出されたデータ部分を、第2送信バッファ28から読み出したデータ、すなわち実施の形態1に説明した符号化処理が施されたデータに置換する処理をおこなう。

【0125】

一方、フレームバッファ52は、受信したデータ、特にアプリケーション層以下の階層に位置するTCPデータやIPデータが含まれた状態のデータフレームを受け取って保持する記憶部である。また、データフレーム抽出処理部54は、フレームバッファ52に保持されたデータフレームから、HTTPデータ等のアプリケーション層に位置するデータを抽出し、抽出したデータを第1受信バッファ38に書き込む処理をおこなう。

【0126】

そして、データフレーム置換処理部56は、フレームバッファ52に保持されたデータフレームのうちデータフレーム抽出処理部54によって抽出されたデータ部分を、第2受信バッファ32から読み出したデータ、すなわち実施の形態1に説明した復号化処理が施されたデータに置換する処理をおこなう。

【0127】

これによって、クライアントやサーバで生成された通信データのうち、通信機器の制御に影響されないデータ部分のみに対して、実施の形態1に説明した符号化／復号化処理をおこなうことができる。

【0128】

つぎに、図8において、システム管理者がクライアント250をもちいて社内LAN220のWWW・DNS・メールサーバ222のファイル管理をおこなう

場合の動作について説明する。まず、システム管理者は、所定のアプリケーション・プログラムによってデータ防護処理装置252の機能を切り離しておく。すなわち、クライアント250は、実施の形態1に説明した符号化／復号化処理を実行することなく、TA／モデム254を介した通常の通信をおこなう状態となる。

【0129】

この状態で、クライアント250は、インターネット・サービス・プロバイダ210のアクセスサーバ214に対してダイヤルアップ接続をおこなうとともに、アクセスサーバ214からユーザ認証を受けることで、インターネット100との接続を確立する。

【0130】

そして、システム管理者は、WWWブラウザを介して、社内LAN220のWWW・DNS・メールサーバ222のURL (Uniform Resource Locator) を入力する。これによって、クライアント250は、WWWページ送信要求を示した送信データをTA／モデム254に送信する。

【0131】

TA／モデム254に送信された送信データは、公衆回線260を介してインターネット・サービス・プロバイダ210のTA／モデム216に到達し、アクセスサーバ214およびルータR30を介して、インターネット100のバックボーンへと伝送される。

【0132】

インターネット100のバックボーンへと伝送された送信データは、インターネット・サービス・プロバイダ110のルータR10に到達し、社内LAN220のルータR40へと到達する。ルータR40に到達した送信データは、LANボード226を介して、WWW・DNS・メールサーバ222に到達する。なお、この際、データ防護処理装置224は、WWW・DNS・メールサーバ222によって、その機能が切り離されている。

【0133】

そして、WWW・DNS・メールサーバ222は、WWWサーバ部分が管理す

るホームページを示すデータを、上記した経路と逆の経路を辿ってクライアント 2 5 0 に返信する。

【0 1 3 4】

ホームページを示すデータを受け取ったクライアント 2 5 0 は、そのホームページを WWW ブラウザ上に表示し、この状態で、システム管理用の特別なコマンドを入力する。このコマンドは、上記同様の経路で WWW・DNS・メールサーバ 2 2 2 に到達する。この際、クライアント 2 5 0 は、上記した所定のアプリケーション・プログラムによってデータ防護処理装置 2 5 2 の機能を有効にする。また、WWW・DNS・メールサーバ 2 2 2 においても、上記コマンドを受け取ると、データ防護処理装置 2 2 4 の機能を有効にする。

【0 1 3 5】

したがって、これ以降のクライアント 2 5 0 と WWW・DNS・メールサーバ 2 2 2 との通信は、実施の形態 1 に説明した符号化／復号化処理を経由しておこなわれることになり、他のクライアントを利用している者が、システム管理者をなりすまして WWW・DNS・メールサーバ 2 2 2 にアクセスすることはできない。

【0 1 3 6】

以上に説明したように、実施の形態 3 にかかるデータ防護処理装置およびデータ防護処理方法によれば、社外のクライアント 2 5 0 側と社内の WWW・DNS・メールサーバ 2 2 2 側のそれぞれに実施の形態 1 で説明したデータ防護処理装置を付加してそれらデータ防護処理装置を発動させることによって、二者間のみにおいて正常な通信が可能になるので、WWW・DNS・メールサーバ 2 2 2 に対しては、データ防護処理装置を有するクライアントのみがアクセス可能となり、他のクライアントからの不正侵入を防止することができる。

【0 1 3 7】

なお、以上の実施の形態 3 においては、社外から社内 LAN 2 2 0 にアクセスする場合を示したが、社内 LAN 2 2 0 から WWW・DNS・メールサーバ 2 2 2 にアクセスする場合においても、図 8 に示すように、システム管理者が使用するクライアント 2 3 0 と、LAN ボード 2 3 4 との間にデータ防護処理装置 2 3

2を配置することで、上記同様の作用および効果を享受することができる。

【0138】

また、以上に説明した実施の形態2，3にかかるデータ防護処理装置においては、実施の形態1において説明したのと同様に、一種類だけの防護キー値を設定していたが、複数の値から構成されるデータパターンを用意しておき、付加範囲の先頭から順に、そのデータパターンが順次示す値を、加算または減算してもよい。

【0139】

また、以上に説明した実施の形態3にかかるデータ防護処理装置においては、実施の形態1において説明したのと同様に、付加条件／付加範囲／防護キー記憶部30に記憶される付加条件、付加範囲および防護キー値は、外部より書き換え可能にすることもできる。

【0140】

また、以上に説明した実施の形態1～3にかかるデータ防護処理方法は、ハードディスクやCD-Rドライブ等の記憶媒体にコンピュータプログラムとして記録することにより提供してもよく、その場合は、上述したデータ防護処理装置に代わって、そのコンピュータプログラムが符号化／復号化処理を実行する。

【0141】

【発明の効果】

以上説明したように、この発明にかかるデータ防護処理装置によれば、受け取ったデジタルデータが所定の数値であるか否かを判定し、所定の数値であると判定された場合には、その判定後に所定の回数のデジタルデータを受け取った際のそのデジタルデータに対して所定の演算値を加算または減算することによって符号化／復号化を実現するので、送受信する一連のデジタルコンテンツのデジタルデータのすべてを受け取らずとも、実際に受け取った部分から順に符号化／復号化を実行することが可能になり、送信／受信バッファとして大容量のものを必要とすることなく、装置構成を安価にすることができる。また、このデータ防護処理装置を互いに有する二者間においては、データの機密化と高速な送受信をともに実現することができる。

【図面の簡単な説明】

【図 1】

実施の形態 1 にかかるデータ防護処理装置の概略構成を示すブロック図である。

【図 2】

実施の形態 1 にかかるデータ防護処理装置の符号化処理を示すフローチャートである。

【図 3】

実施の形態 1 にかかるデータ防護処理装置において、防護キー値の加算処理を説明するための説明図である。

【図 4】

符号化処理によって得られるバイトデータ列の例を示す図である。

【図 5】

実施の形態 1 にかかるデータ防護処理装置の復号化処理を示すフローチャートである。

【図 6】

実施の形態 2 にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。

【図 7】

実施の形態 2 にかかるデータ防護処理装置およびデータ防護処理方法において、データ防護機能付きモデムの一例を示すブロック図である。

【図 8】

実施の形態 3 にかかるデータ防護処理装置およびデータ防護処理方法の適用例を示すシステム構成図である。

【図 9】

実施の形態 3 にかかるデータ防護処理装置の概略構成を示すブロック図である。

【符号の説明】

1 0, 2 0, 2 2 4, 2 3 2, 2 5 2 データ防護処理装置

- 2 2 第 1 送信バッファ
- 2 4 防護キー付加位置判定部
- 2 6 防護キー付加処理部
- 2 8 第 2 送信バッファ
- 3 0 付加条件／付加範囲／防護キー記憶部
- 3 2 第 2 受信バッファ
- 3 4 防護キー除去処理部
- 3 6 防護キー除去位置判定部
- 3 8 第 1 受信バッファ
- 4 2, 5 2 フレームバッファ
- 4 4, 5 4 データフレーム抽出処理部
- 4 6, 5 6 データフレーム置換処理部
- 1 0 0 インターネット
- 1 1 0, 2 1 0 インターネット・サービス・プロバイダ
- 1 2 0, 2 2 0 社内 LAN
- 1 2 2, 2 2 2 WWW・DNS・メールサーバ
- 1 2 4, 2 1 4 アクセスサーバ
- 1 2 6, 1 3 2 データ防護機能付 TA／モデム
- 1 2 8, 1 3 0, 2 3 0, 2 3 8, 2 5 0 クライアント
- 1 4 0, 2 6 0 公衆回線
- 1 5 1 バッファ
- 1 5 2 データ圧縮部
- 1 5 3 フレーム処理部
- 1 5 4 変調処理部
- 1 5 5 D／Aコンバータ
- 1 6 1 バッファ
- 1 6 2 データ解凍部
- 1 6 3 データ抽出処理部
- 1 6 4 復調処理部

165 A/Dコンバータ

212, 222 WWW・DNS・メールサーバ

216, 254 TA/モデム

226, 234 LANボード

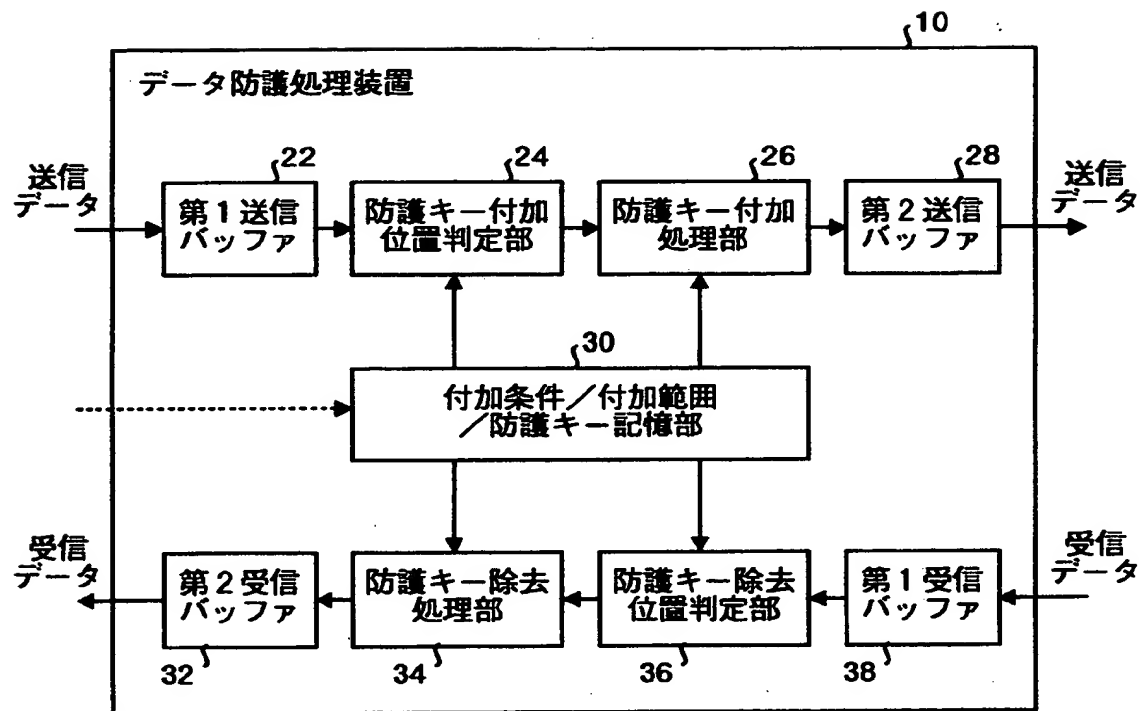
236 DNS・メールサーバ

240 プロキシサーバ

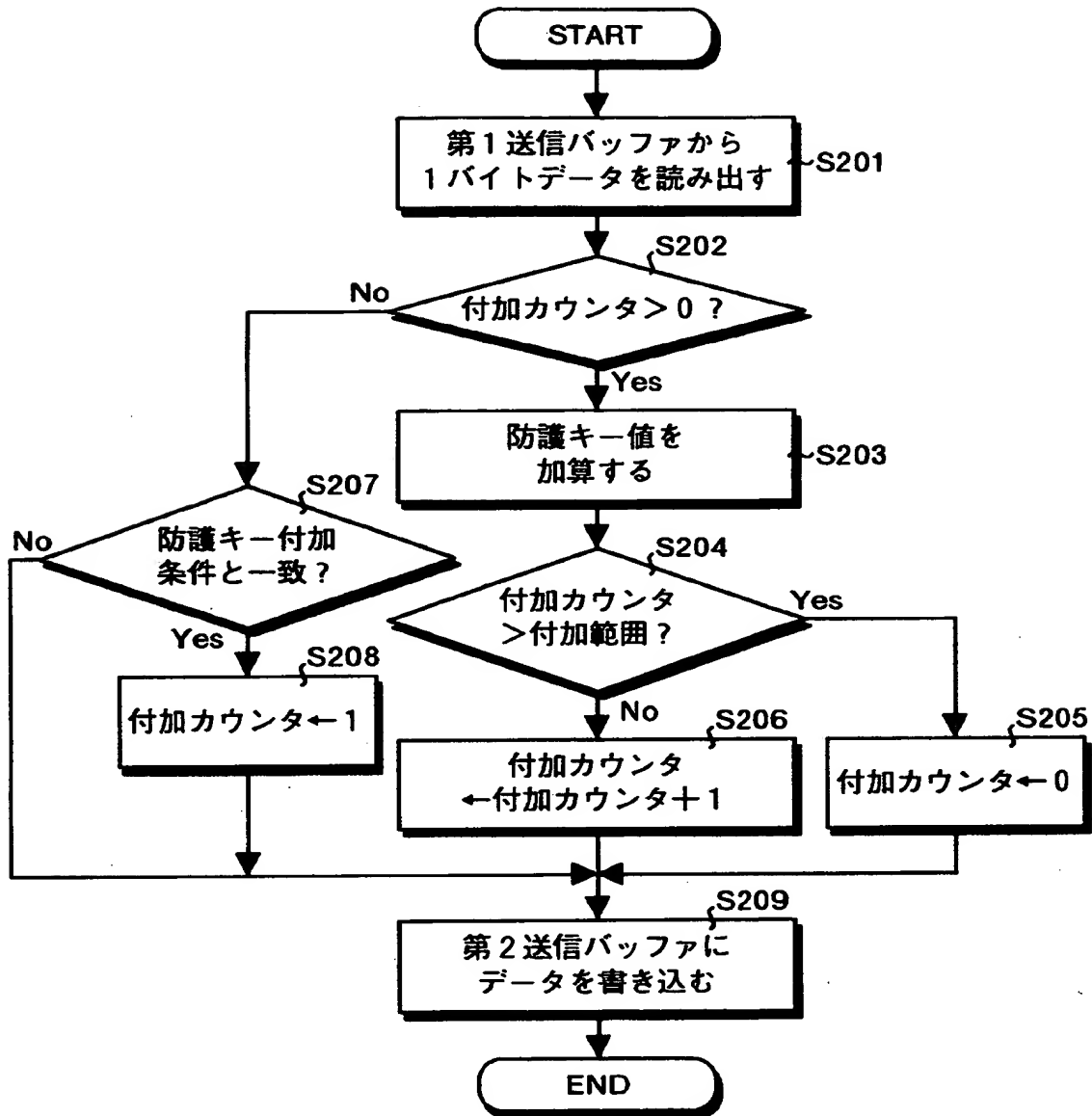
R10, R20, R30, R40 ルータ

【書類名】 図面

【図 1】

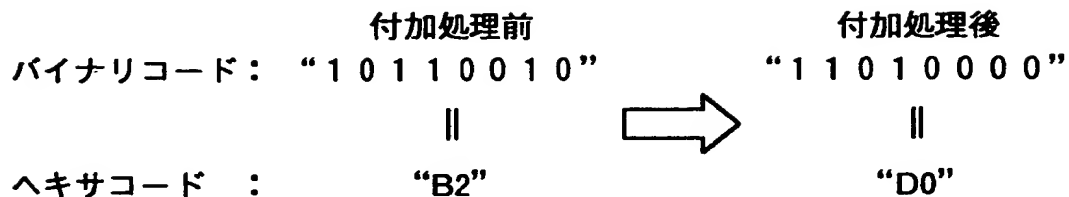


【図 2】



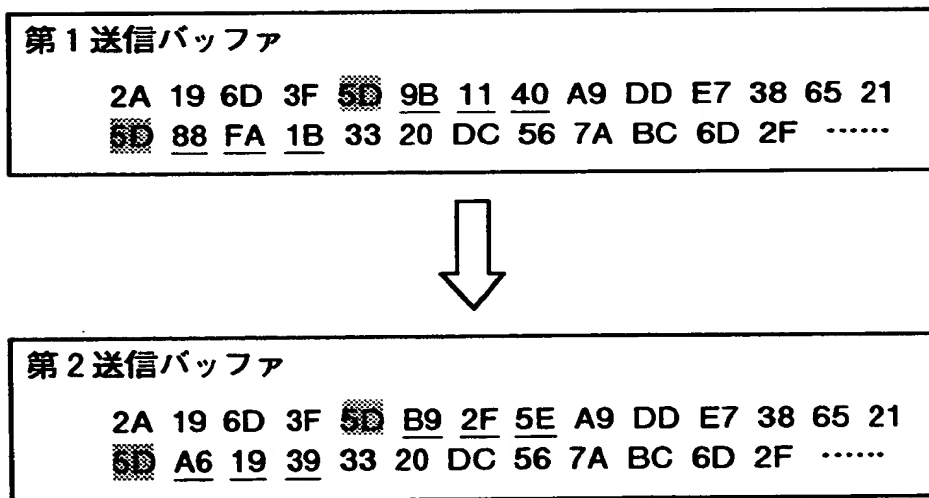
【図 3】

「防護キー値 = “1E” の場合」

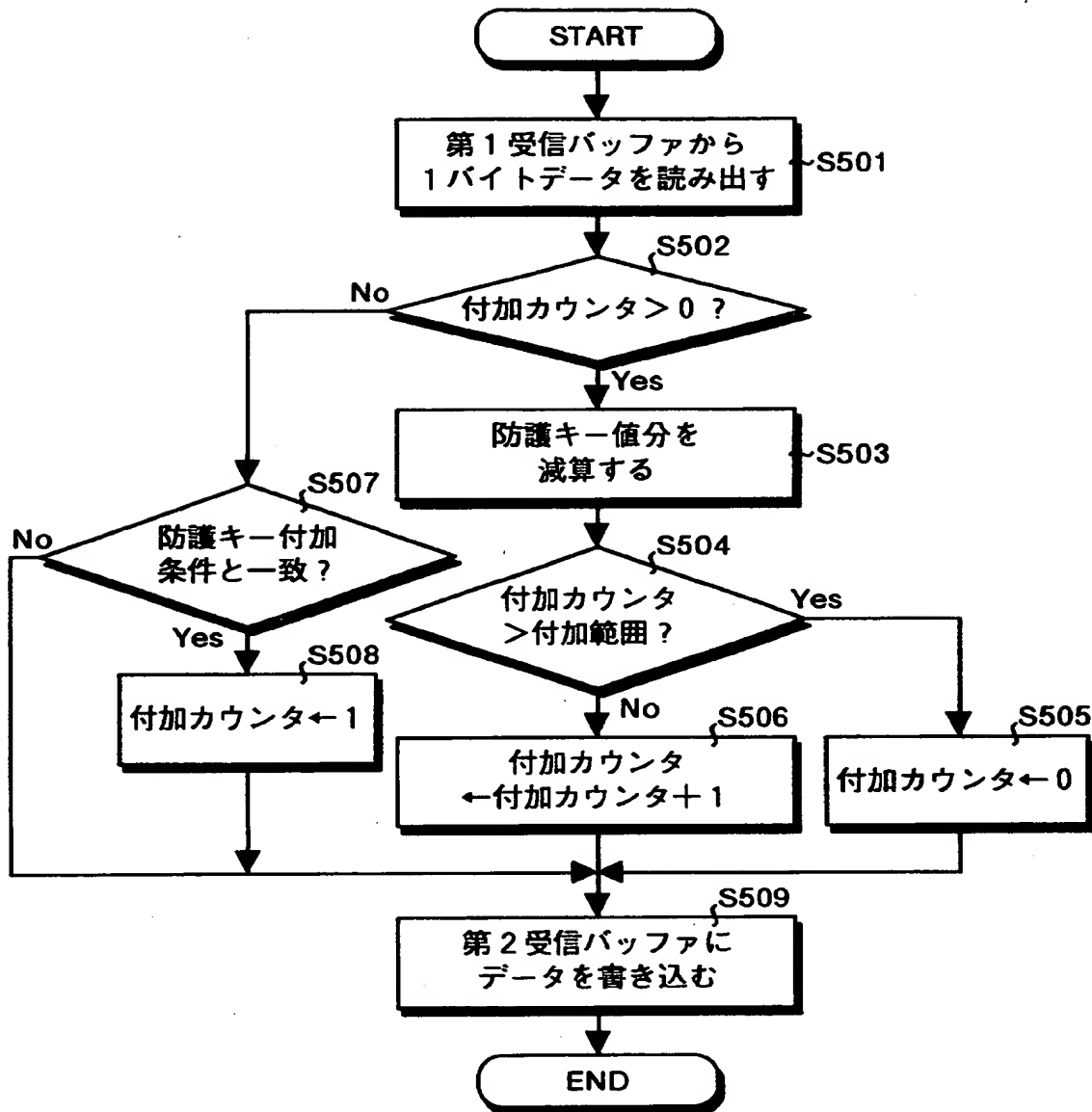


【図 4】

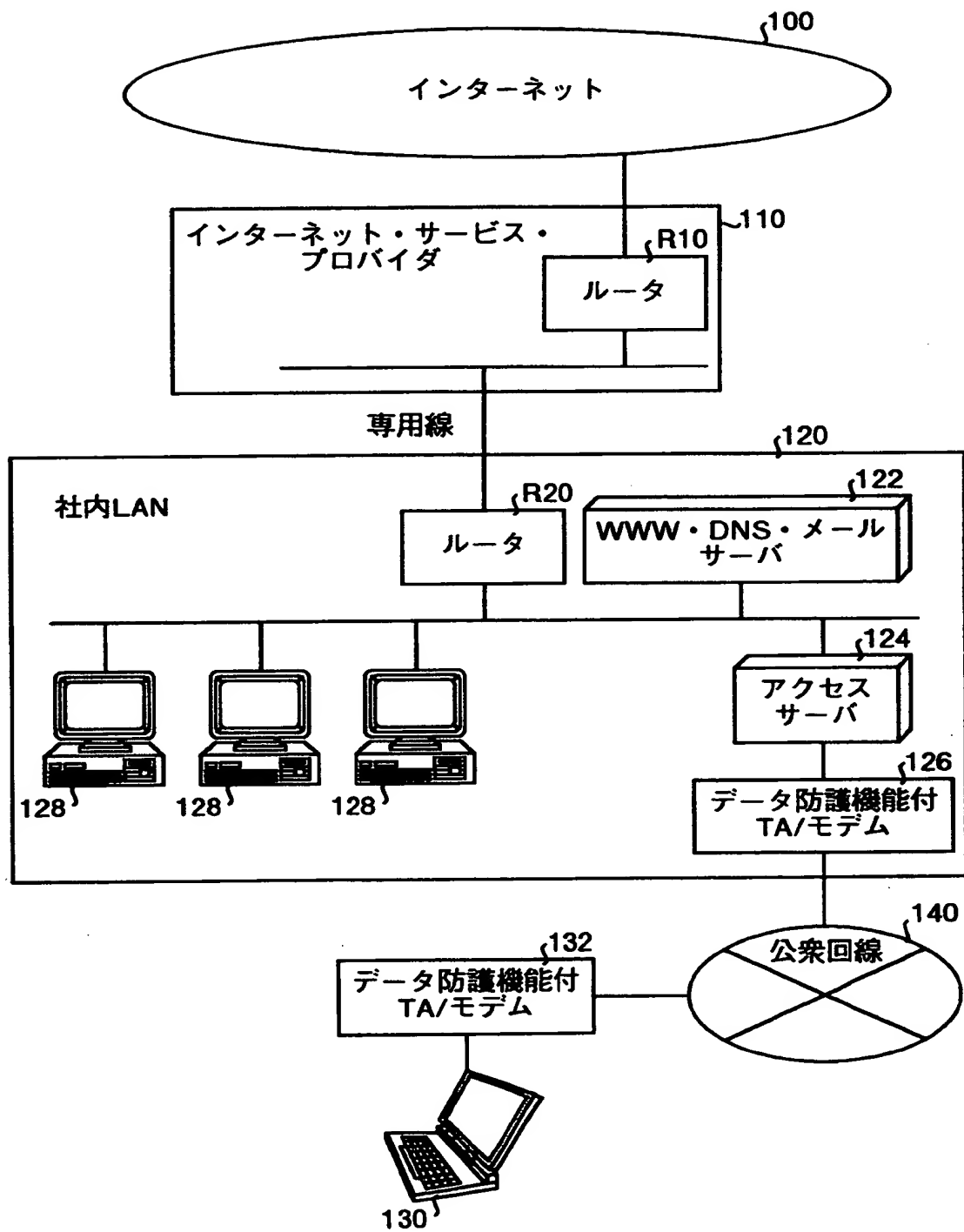
付加条件 : “5D” のつぎから
 防護キー値 : “1E”
 付加範囲 : 3 バイト



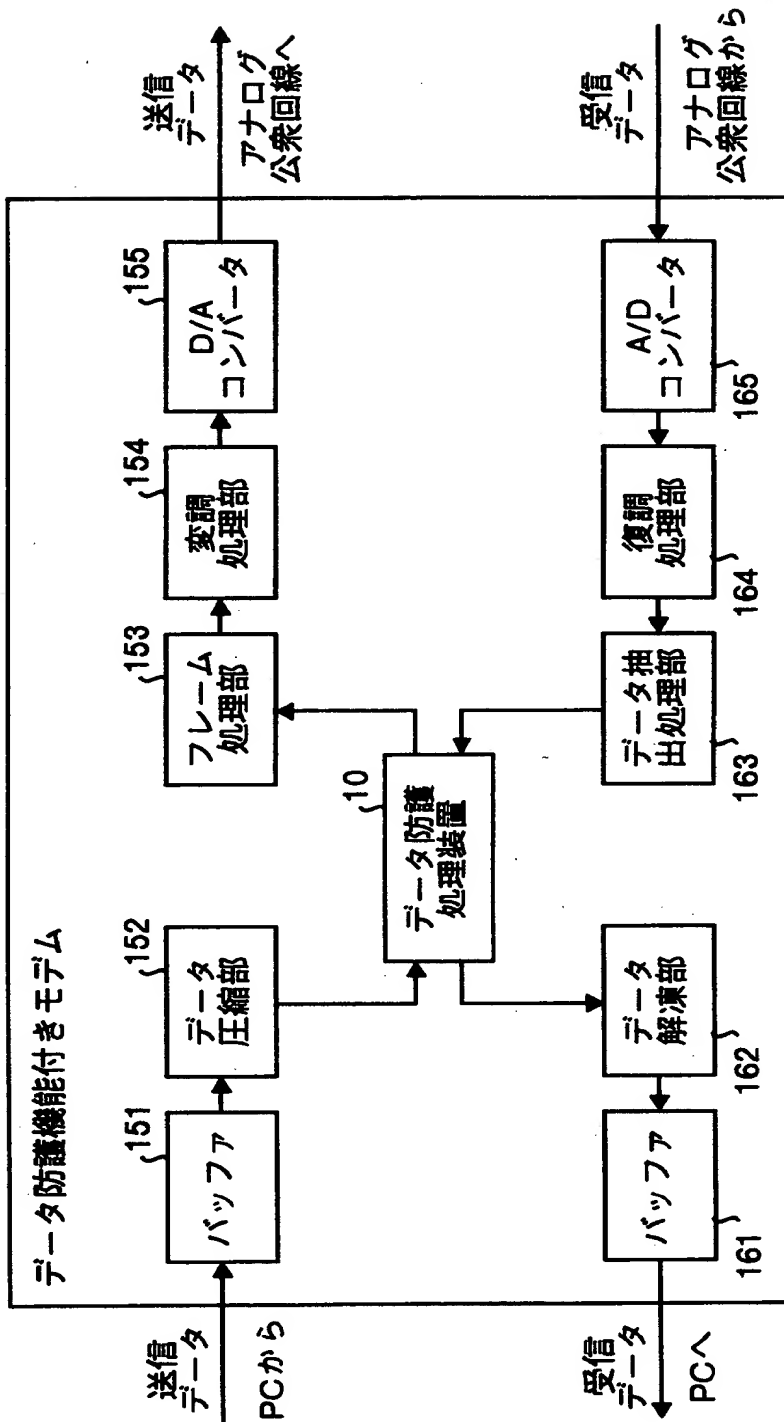
【図 5】



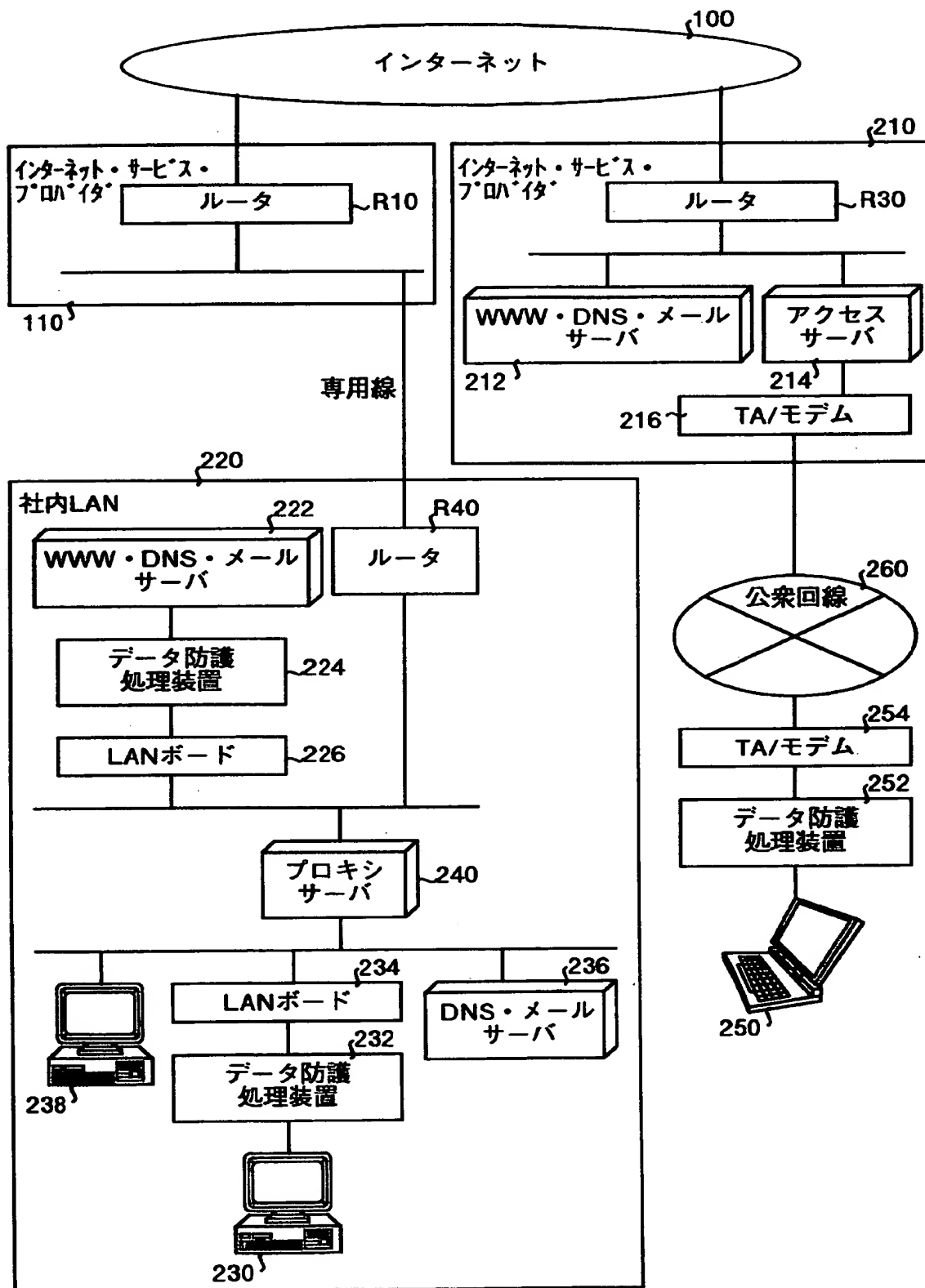
【図6】



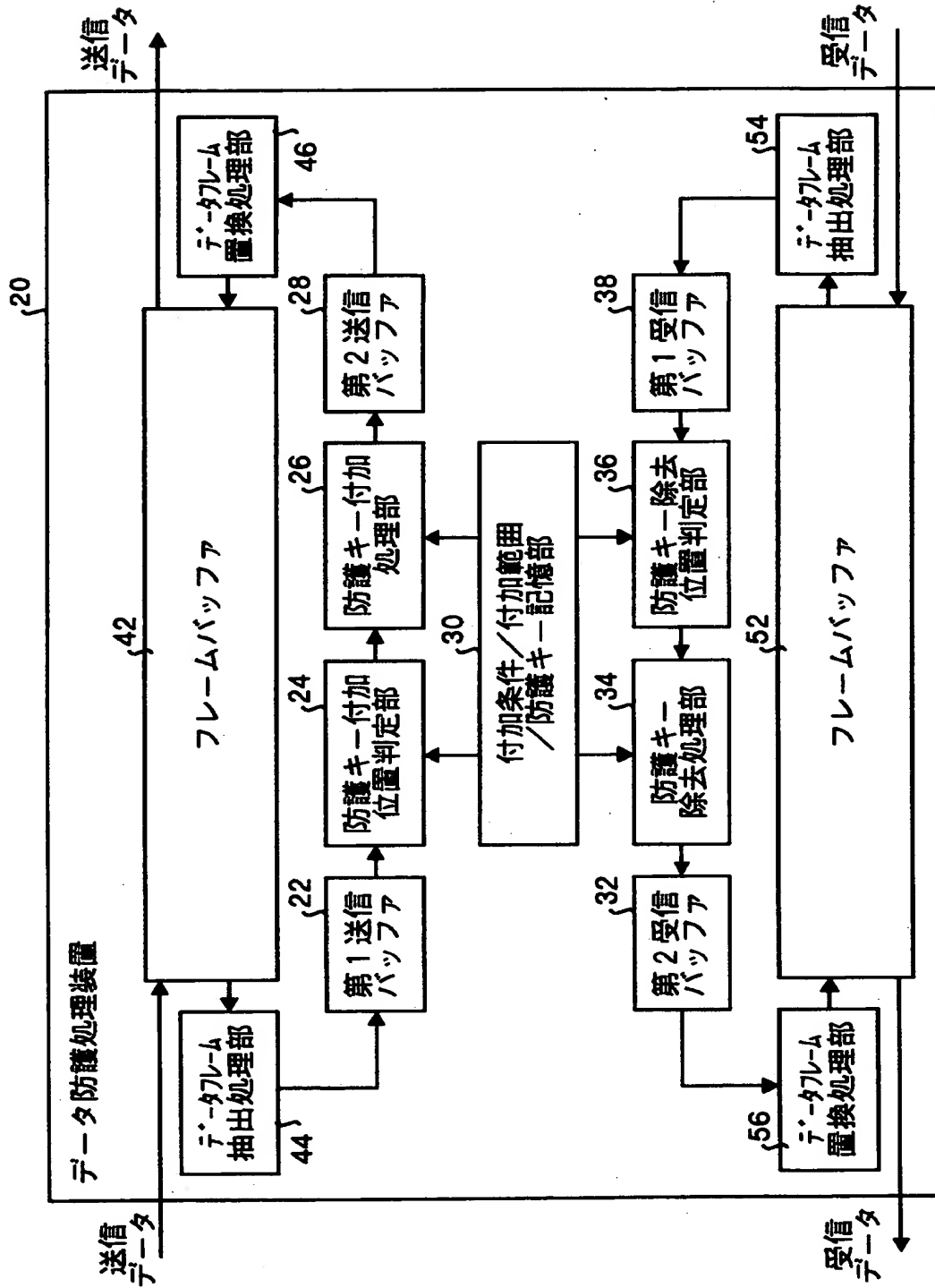
【図 7】



【図 8】



【図 9】



【書類名】 要約書

【要約】

【課題】 送受信データをそのデータ・サイズを増大させることなくかつ十分な保安性を高めて符号化／復号化するデータ防護処理装置を提供すること。

【解決手段】 防護キー付加位置判定部 2 4 または防護キー除去位置判定部 3 6 において、受け取ったデジタルデータが所定の付加条件を満たすか否かを判定し、所定の付加条件を満たす場合には、防護キー付加処理部 2 6 または防護キー除去処理部 3 4 において、その判定後に所定の回数のデジタルデータを受け取った際のそのデジタルデータに対して所定の防護キー値を加算または減算することによって符号化／復号化を実現する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [300023383]

1. 変更年月日 2000年 3月16日

[変更理由] 新規登録

住 所 徳島県徳島市川内町平石住吉209番地5
氏 名 株式会社トリニティーコミュニケーション

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.